

FEDERAL TRADE COMMISSION

July 11-12, 2007

SPAM

SUMMIT

THE NEXT GENERATION OF THREATS AND SOLUTIONS

Uncovering the Malware Economy

Moderator:

Sheryl L. Drexler, Investigator,
Division of Marketing Practices, FTC

- What are the financial incentives for malicious spammers? What is the cost along the email chain to consumers, businesses, Internet service providers, and networks?

Uncovering the Malware Economy

- **Gregory Crabb**, United States Postal Inspector, United States Postal Inspection Service
- **Jens W.L. Hinrichsen**, Product Marketing Manager, Consumer Solutions, RSA, The Security Division of EMC
- **Andrew J. Klein**, Senior Product Marketing Manager, SonicWALL, Inc.
- **Heinan Landa**, President and Founder, Optimal Networks, Inc.

Andrew J. Klein

- Senior Product Marketing Manager,
SonicWALL, Inc.

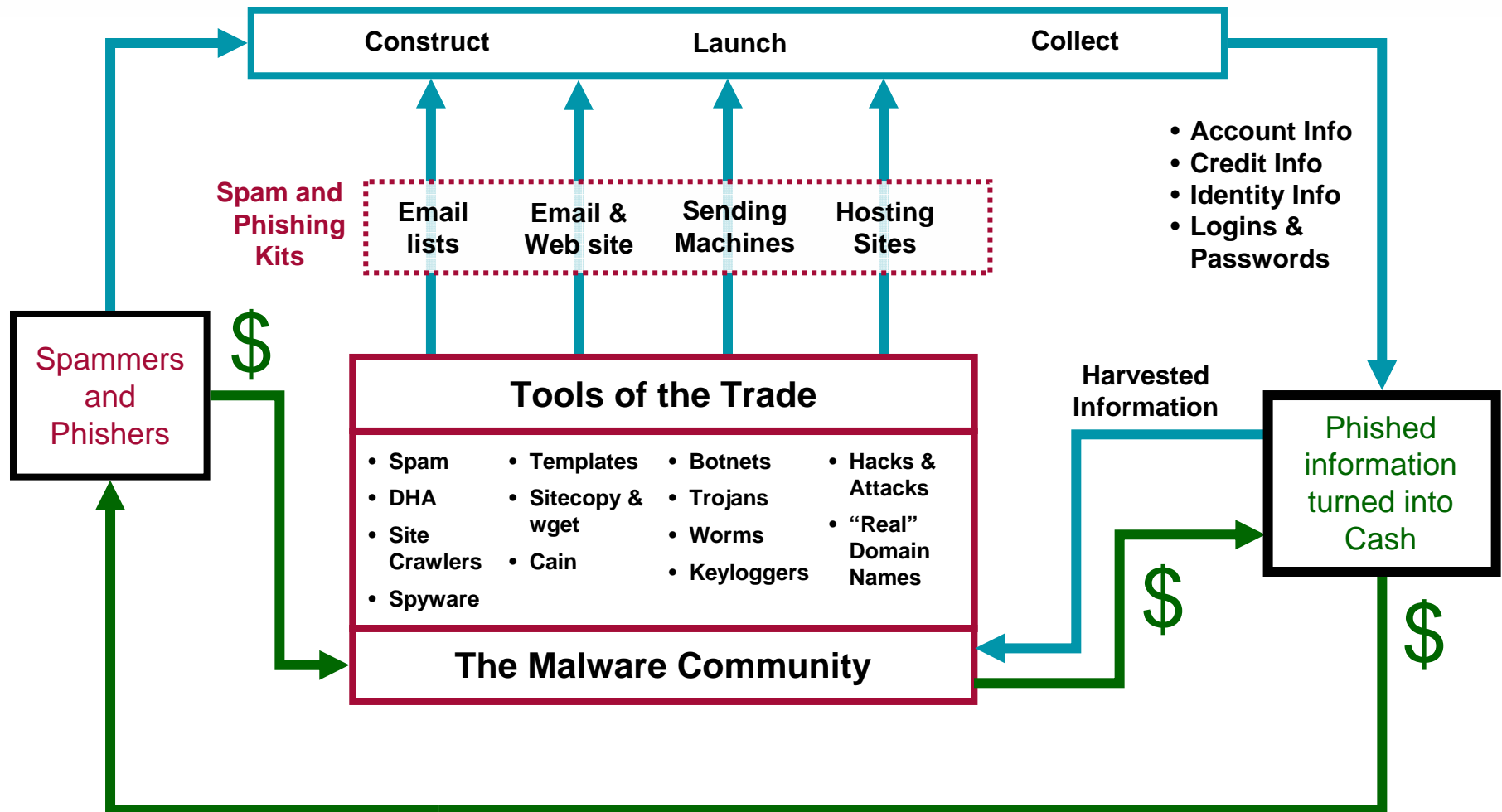
Malware, Mayhem & Money The Rise of the Malware Economy

Andrew Klein

Senior Product Marketing Manager



The Malware Economy



Tools of the Trade – Botnets

A collection of compromised computers that are run under a common control structure

- **Functions**

- Spam, phishing, pharming, distributing adware or malware, DHA, DOS attacks, and temporarily storing illegal, malicious or stolen files.

- **Create your own**

- Mr. X (Dutch Spammer) – 600 to 700 machines, 9B spam emails

- **Rent one out for \$300 to \$700 per hour**

- Jeanson James Ancheta (19) – \$60,000 in 6 months
- Christopher Maxwell (19) – \$100,000 in one year

- **How many**

- 70 Million compromised machines (Trend Micro)
- 100 to 150 Million compromised machines (Vint Cerf)
- Over 10,000 botnets become active each day (Symantec)
- 8 to 9 million compromised machines become active each month (Trend Micro)

Tools of the Trade - Domains

- citibank-validate.info
- earthlink-reactivation.net
- services-bankofamerica.com
- sales-aol.net
- secure-ebay.com
- msn-reactivation.net
- secure-usbank.info
- service-visa.net
- verification-e-gold.com
- rewardprogramsurvey.us
- customer-verification.com
- banking-account-renewal.com

Hall of Fame

Phishers SSL Certificate

>> citibanhk.de <<

Duplicated Registrar Info

>> credtlyonaisse.com <<

Registering a Cyrillic “a”

>> paypal.com <<

Tools of the Trade – Hacks

Hacked bank server hosts phishing sites

Direct

Criminals hack a Chinese bank's server and use it to host phishing sites.

By Jeremy Kirk, IDG News Service, 03/13/06

Criminals appear to have hacked a Chinese bank's server and are using it to host phishing sites from customers of eBay and a major U.S. bank, according to Internet security experts.

It may be the first scheme that uses one bank's infrastructure to expose its customers to phishing services developer for Netcraft, based in Bath, England.

A user of Netcraft's free phishing toolbar reported receiving a suspicious email with links to sites located in hidden directories on a server with IP addresses belonging to the Chinese Construction Bank, a state-owned bank with more than 14,000 branches in China.

One of the phishing sites offered customers of Chase Bank, part of JPMorgan Chase & Co., a survey. The survey asked for the user's ID and password. Another site requested the person's bank card number, PIN, card verification number and Social Security number, Netcraft said.

Press Release

Goldleaf Technologies Responds to Phishing Attempt

BRENTWOOD, Tenn., May 27, 2006 (BUSINESS WIRE) -- Goldleaf Technologies, a unit of Goldleaf Financial Solutions, Inc. (NASDAQ:GFSI) and a leading provider of Web-based ACH and check conversion solutions, announced today that it has identified and responded to attempts to redirect users to fraudulent Web sites.

On Thursday, May 25, Goldleaf Technologies' IT staff identified an attempt to redirect its clients' customers to a phishing website to entice them to enter their personal financial information. To ensure the security of the network, the company temporarily suspended all Internet access to Goldleaf Technologies' Web site services.

Florida banks hacked in new spoofing attack

Hackers use legitimate Web sites for phishing attacks on three Florida banks, making it harder for even savvy users to detect the scam.

By [Robert McMillan](#), IDG News Service, 03/30/06

Three Florida banks have had their Web sites compromised by hackers in an attack that security experts are calling the first of its type.

Earlier this month, attackers were able to hack servers run by the ISP that hosted the three banks' Web sites. They then redirected traffic from the legitimate Web sites to a bogus server, designed to resemble the banking sites, according to Bob Breeden, special agent supervisor with the Florida Department of Law Enforcement's Computer Crime Center.

Users were then asked to enter credit card numbers, PINs and other types of sensitive information, he said.

and corrected the problem. We added additional security in addition to contacting our customers and law enforcement authorities.

Service

Hosted

SONICWALL

Making money with Tools

Spyware kits for sale - £10 or \$17

A Russian website has appeared on the internet selling spyware kits for ten pounds.

The spyware kit, called WebAttacker, is currently available for approximately £10 (\$17). The website, which refers to its creators only as spyware and adware developers, touts the strengths of its software and makes the kits available for purchase online - even offering buyers technical support.

Included in the kits are scripts designed to simplify infecting computers. The buyer only needs to send spam to email addresses inviting recipients to visit a compromised website.

China detains 6 over 'panda' virus

BEIJING, China (Reuters) – China has detained six men in their 20s for writing or profiting from a computer virus dubbed the "joss-stick burning panda" which has infected over a million PCs in the country, local media said on Wednesday.

The worm wreaked havoc among individual and corporate users in China in a late 2006 outbreak, deleting files, damaging programs and attacking web portals.

It got its name from changing icons on desktops into cute cartoon pandas, the most famous of which holds three burning joss-sticks in his paws.

Chinese media have said that the worm was able to steal account names of online gamers and instant messengers, which are hotly traded with real money in China's cyberspace.

Police held Li Jun, 25 a native of Wuhan city in central China, who wrote the virus in October and had earned more than 100,000 yuan (\$12,890) by selling it to about 120 people, the Beijing News said.

The other five, from three different provinces, were detained for updating and spreading the virus or for profiting from the stolen account names, the Beijing News said.

"It is the first time our country has cracked a major computer virus case," it added.

Tools 2.0

Quality, quantity of phishing kits on the rise

By Munir Kotadia

Mon Oct 16 12:20:10 PDT 2006

The marketplace for phishing toolkits, which can allow technophobe criminals to quickly and easily set up spoofed versions of banking Web sites, is booming, with kits changing hands for as little as \$30.

Although phishing kits are nothing new, in the past year their quantity and quality have increased dramatically, according to Dan Hubbard, vice president of security research for Websense and a representative of the Anti-Phishing Working Group.

Phishing kits "have been around for years, but the volume is one of the big changes," Hubbard said. "The kits available are better designed."

In particular, Hubbard noted that the kits were vaunting their immunity to common defensive techniques. These include detection by signature-based defensive programs, which look for the signature, or the "fingerprint," of known malicious software. Another is heuristics, which use pattern recognition to identify threats.

Phishing Toolkit being Sold Online

Techtree News Staff

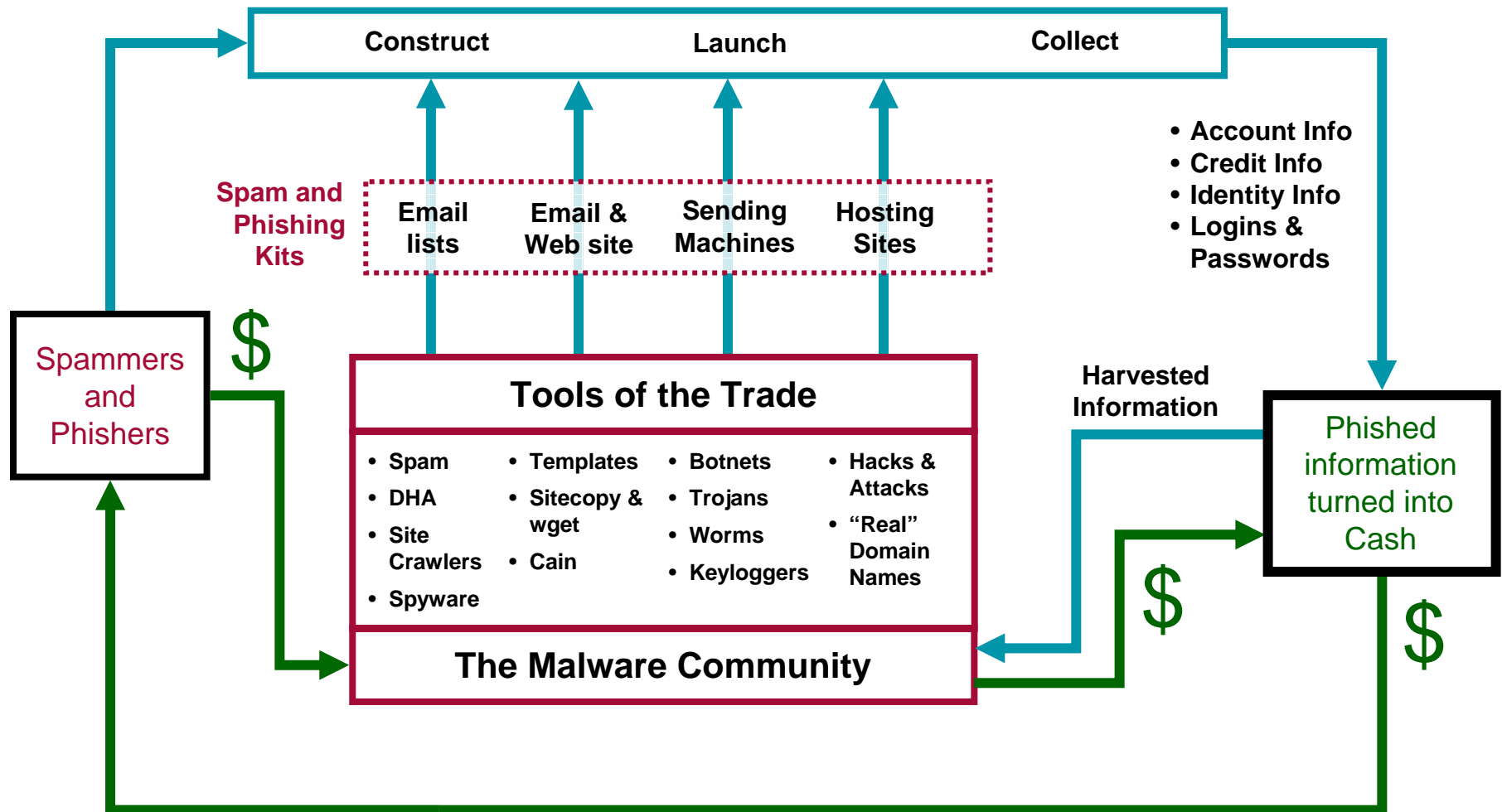
Jan 15 2007

RSA, the security division of EMC, has announced that its Anti-Fraud Command Centre (AFCC) has uncovered a new phishing toolkit being sold and used online by fraudsters.

The company said that this new phishing kit, dubbed as 'Universal Man-in-the-Middle Phishing Kit', is designed to facilitate new and sophisticated attacks against global organizations in which victims communicate with a legitimate Web site via a fraudulent URL set by the fraudster. This allows the fraudster to capture victims' personal information in real-time.

In a statement, Marc Gaffan, Executive of RSA, said that what is unique about this kit is that it changes the rules of the game. It offers a much better return on investment, and can be used to mount attacks against multiple targets, such as several banks simultaneously, without any code changes or technical expertise. A hacker could employ it against dozens of targets.

The Malware Economy



Uncovering the Malware Economy

- **Gregory Crabb**, United States Postal Inspector, United States Postal Inspection Service
- **Jens W.L. Hinrichsen**, Product Marketing Manager, Consumer Solutions, RSA, The Security Division of EMC
- **Andrew J. Klein**, Senior Product Marketing Manager, SonicWALL, Inc.
- **Heinan Landa**, President and Founder, Optimal Networks, Inc.

Jens W.L. Hinrichsen

- Product Marketing Manager,
Consumer Solutions, *RSA*,
The Security Division of EMC



The Security Division of EMC

Phishing & Crimeware on the Upswing

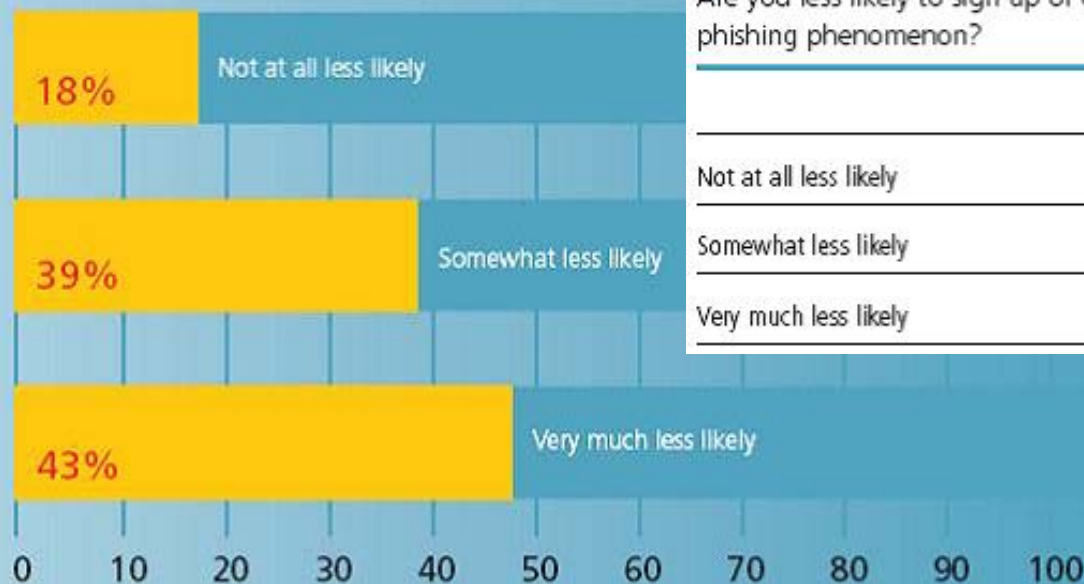
Latest Trends and Perspective

Jens Hinrichsen

RSA, the Security Division of EMC

Consumer Confidence Remains Shaky

Are you less likely to respond to an email from your bank because of the phishing phenomenon?



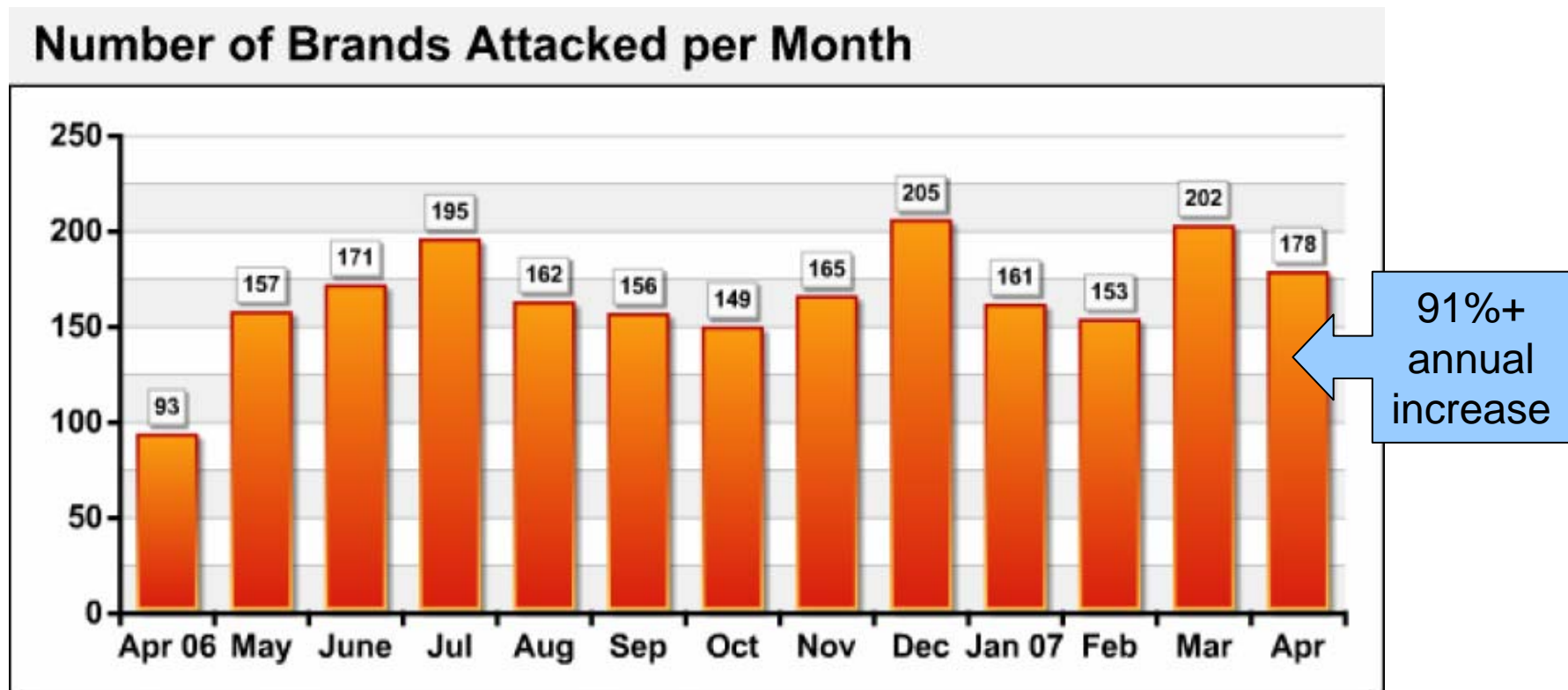
Are you less likely to sign up or continue to use your bank's online services because of the phishing phenomenon?

	November 2004	November 2005	December 2006
Not at all less likely	51%	61%	48%
Somewhat less likely	32%	32%	35%
Very much less likely	17%	7%	17%



The Security Division of EMC

While Phishing Continues to Grow



Source: RSA Anti-Fraud Command Center repository

Some of the (Unfortunate) Latest Trends

- » More institutions than ever being targeted by phishing
 - More FCUs and Regional banks coming under fire
 - More sophisticated attacks
 - Multi-redirectors with SSL certificates
 - Significantly greater use of phishing-based Man-In-The-Middle attacks
 - Tandem phishing and Distributed Denial of Service (DDoS) attacks
 - Spear phishing continue to grow
- » More brazen fraudsters
- » While the use of crimeware/Trojans is growing. . .



The Security Division of EMC

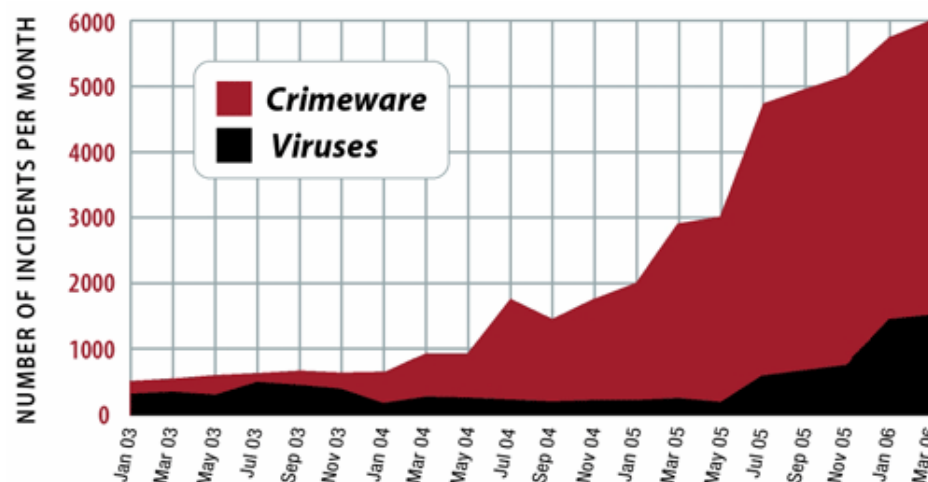
While Crimeware is Taking Off

» Growing at an “unhealthy” clip

- Of the hundreds of thousands of pieces of malicious code in existence worldwide, roughly half of new variants in 2006 were Trojans. . .
- Recent RSA analysis of a single Gozi/BankSniff variant showed 30,000 infected users in a single month

» Some of the crimeware families

- Torpig
- Gozi/BankSniff
- Haxdoor
- Trj/Briz.A (made-to-order)
- Metafisher
- *Not to mention “Super Trojans”. . .*



Source: The Kaspersky Internet Security Lab



The Security Division of EMC

Crimeware and Consumers – Cause for Concern

RSA Consumer Study, 12/06

» “How concerned have you been about other types of attacks, such as trojans and keyloggers over the past six months?”

. . . 44% of respondents already “increasingly concerned”

» *Expected to increase markedly over coming 6-12 months*

According to a recent survey by the National Cybersecurity Alliance, over 90 percent of consumers have some type of spyware on their computers

“Super Trojans”?

The Tools Are Becoming More Capable, Available – And Affordable!

[illegible]

Trojan Promotion in the Underground. . .

The logo for SE-CODE, featuring the text "SE-CODE" in a white, serif font. The text is centered and has a subtle reflection effect below it. The background is dark with a green, grid-like pattern that resembles a wireframe or a digital network.

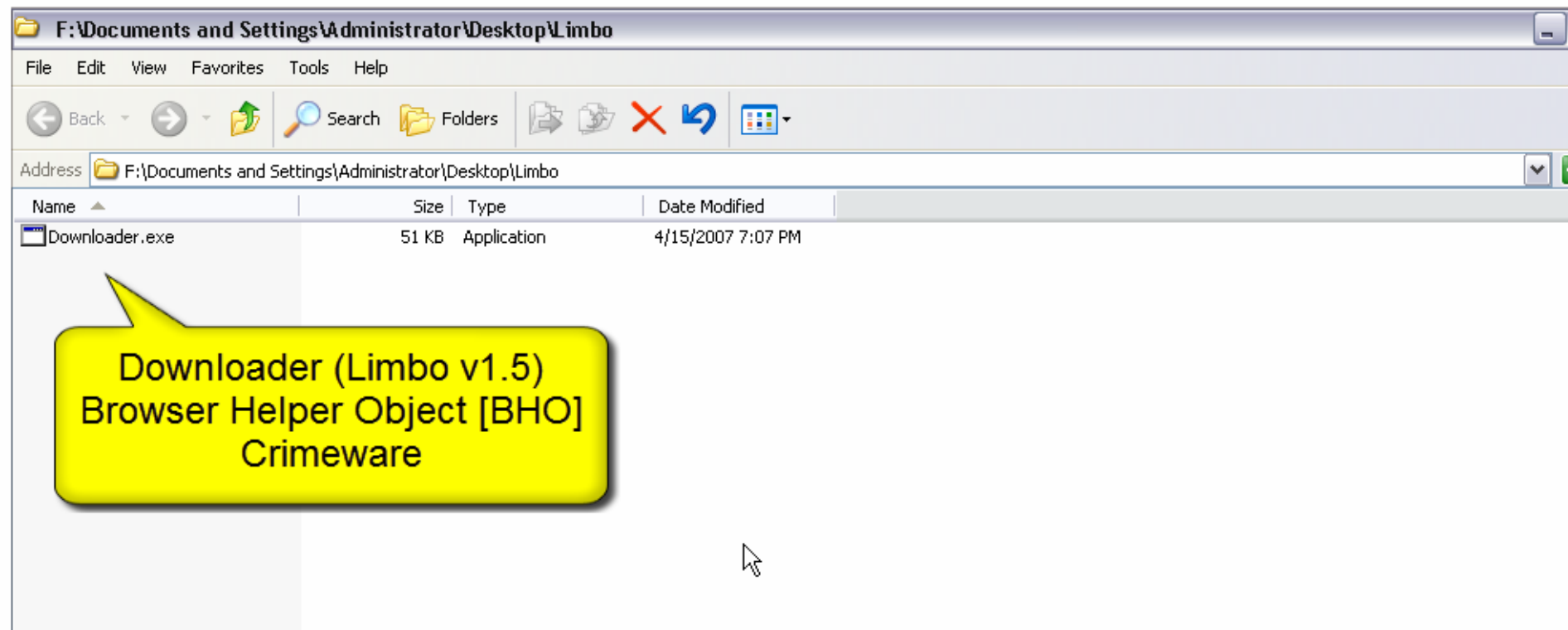
SE-CODE – The E-gold Session-Hijacking Trojan



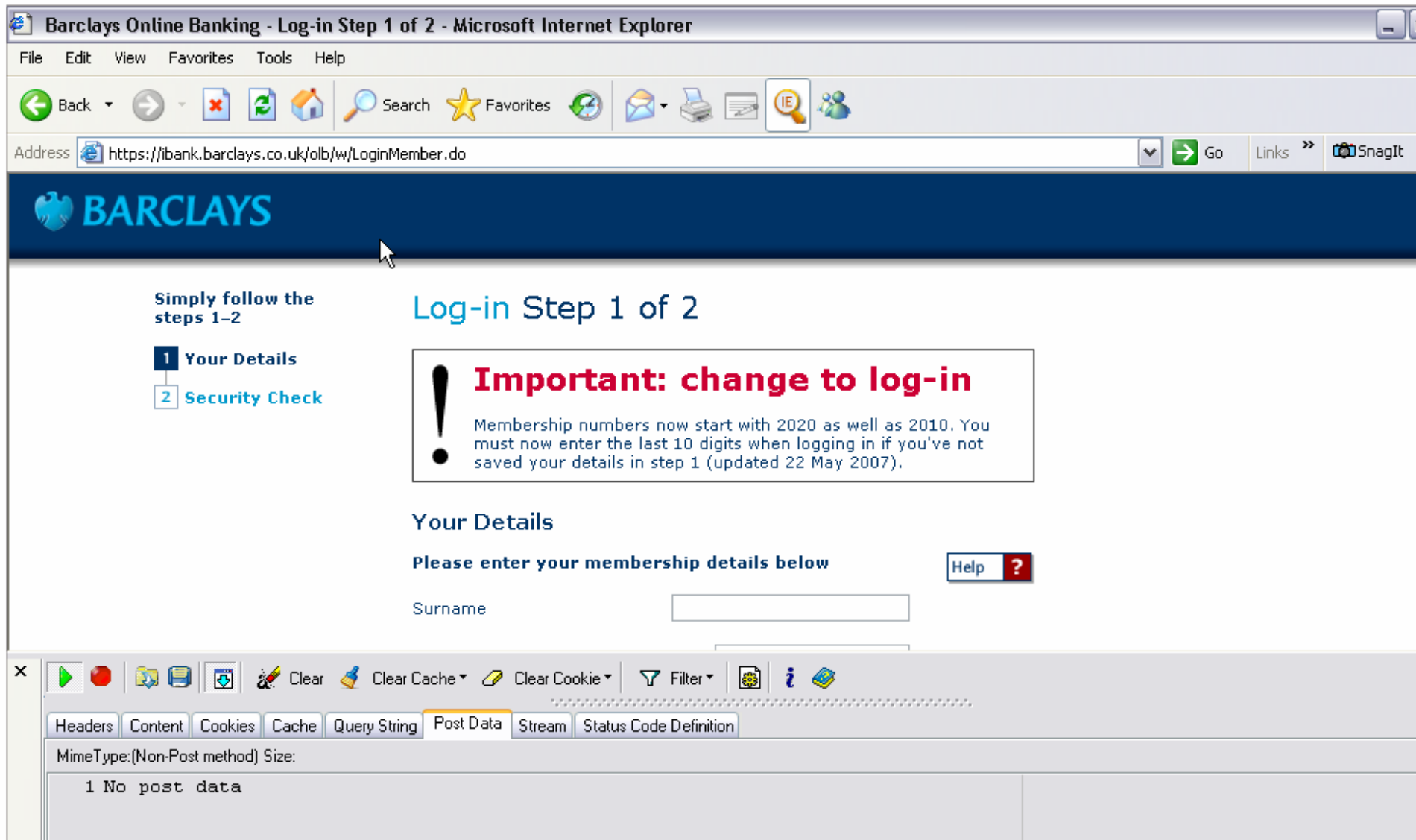
The Security Division of EMC

Sample Financial Trojan (“Limbo”) In Action

» HTML-injection Trojan, targeting additional credentials



Sample Financial Trojan ("Limbo") In Action



Sample Financial Trojan ("Limbo") In Action

Barclays Online Banking - Log-in Step 1 of 2 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Reload Print Mail IE People

Address <https://ibank.barclays.co.uk/olb/w/LoginMember.do> Go Links SnagIt

2 Security Check

Important change to log in

Membership numbers now start with 2020 as well as 2010. You must now enter the last 10 digits when logging in if you've not saved your details in step 1 (updated 22 May 2007).

Your Details

Please enter your membership details below [Help ?](#)

Surname

Membership number 20

[Forgotten your log-in details?](#)

Save time - remember your membership details [Help ?](#)

☐ Select this box and then the **green 'next' button** to save your membership number and surname on this computer.

Clear Clear Cache Clear Cookie Filter


Headers Content Cookies Cache Query String **Post Data** Stream Status Code Definition

MimeType:(Non-Post method) Size:

1 No post data

Sample Financial Trojan (“Limbo”) In Action

2 Security Check

**Important change to log in**

Membership numbers now start with 2020 as well as 2010. You must now enter the last 10 digits when logging in if you've not saved your details in step 1 (updated 22 May 2007).

Your Details

Please enter your membership details below [Help ?](#)

Surname

Membership number 20

[Forgotten your log-in details?](#)

Save time - remember your membership details [Help ?](#)

☐ Select this box and then the **green 'next' button** to save your membership number and surname on this computer.

IE HTTP Analyzer

Clear Clear Cache Clear Cookie Filter

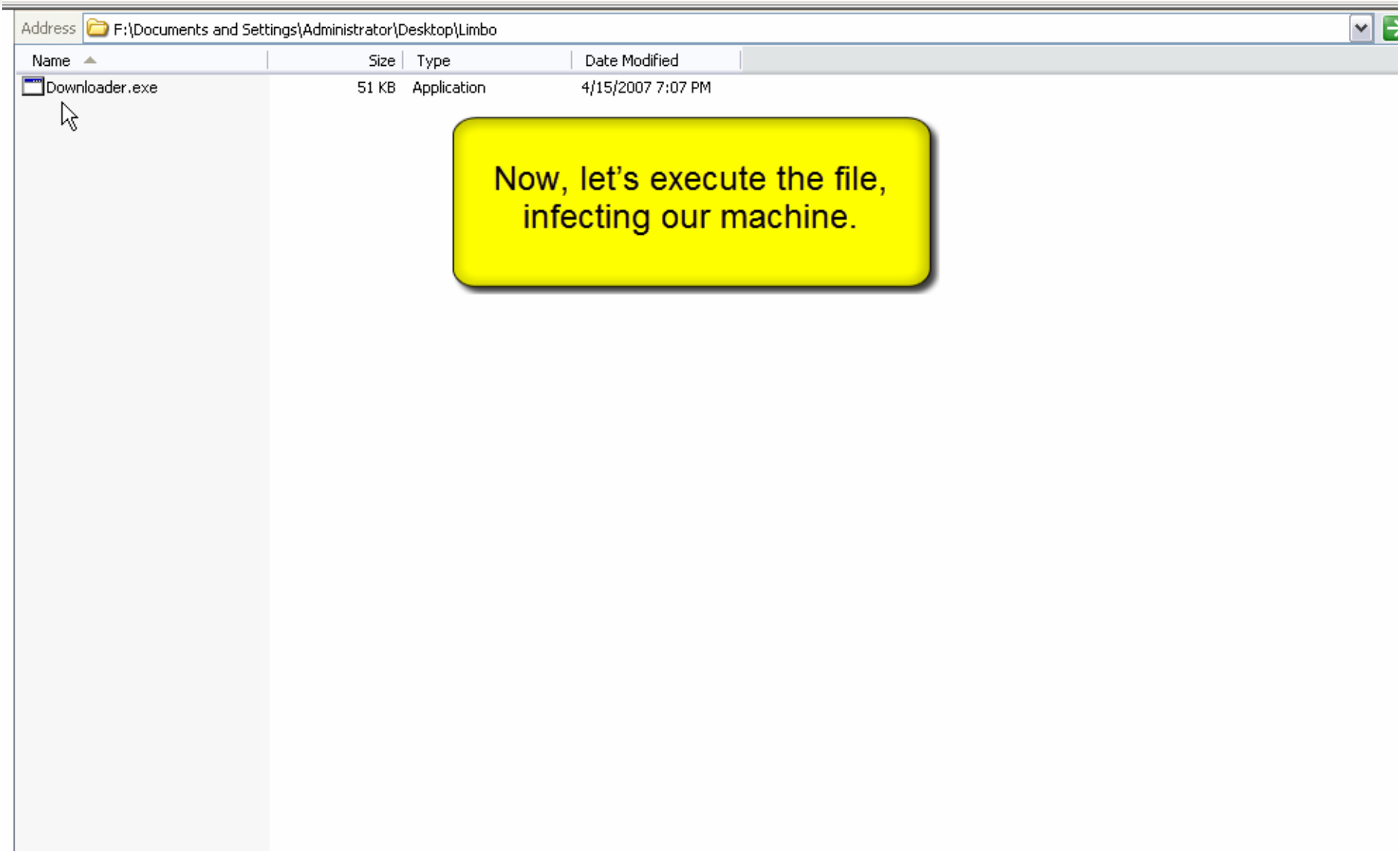
Headers Content Cookies Cache Query String Post Data Stream Status Code Definition

MimeType:(Non-Post method) Size:





1 No post data

Our machine is still clean - everything is as it should be.

Sample Financial Trojan (“Limbo”) In Action




Sample Financial Trojan ("Limbo") In Action

Address  <https://ibank.barclays.co.uk/olb/w/LoginMember.do>  Go  Links  SnagIt

saved your details in step 1 (updated 22 May 2007).

Your Details

Please enter your membership details below  ?


Surname

Membership number 20

ATM Number

ATM Pin

[Forgotten your log-in details?](#)

Save time - remember your membership details  ?

☐ Select this box and then the **green 'next' button** to save your membership number and surname on this computer.

Immediately, we see new fields inside the genuine website, with the genuine URL.

ITTP Analyzer





Clear Clear Cache Clear Cookie Filter

Headers Content Cookies Cache Query String **Post Data** Stream Status Code Definition

MimeType:(Non-Post method) Size:


1 No post data

Sample Financial Trojan ("Limbo") In Action

Address  <https://ibank.barclays.co.uk/olb/w/LoginMember.do>  Go  Links  SnagIt

saved your details in step 1 (updated 22 May 2007).

Your Details


Please enter your membership details below  ?

Surname

Membership number

ATM Number

[log-in details?](#)

remember your membership details  ?

is box and then the **green 'next' button** to
your membership number and surname on this
er.

And our details are then sent
to both the fraudster and to
the bank -- we would log in
successfully

ITTP Analyzer

0 bytes sent to

```
156 Barclays Online Banking - Log-in Step 1 of 2
157 action=Submit+Membership+Number
158 servlet=startlogin
159 screenName=logonMember1i
160 surname=Alex
161 membershipNo=123456789
162 surname=4444333322221111
163 surname=1234
164 Next.x=57
165 Next.v=17
```

0 bytes received by

```
1
```

Sample Financial Trojan ("Limbo") In Action



Sample Financial Trojan (“Limbo”) In Action

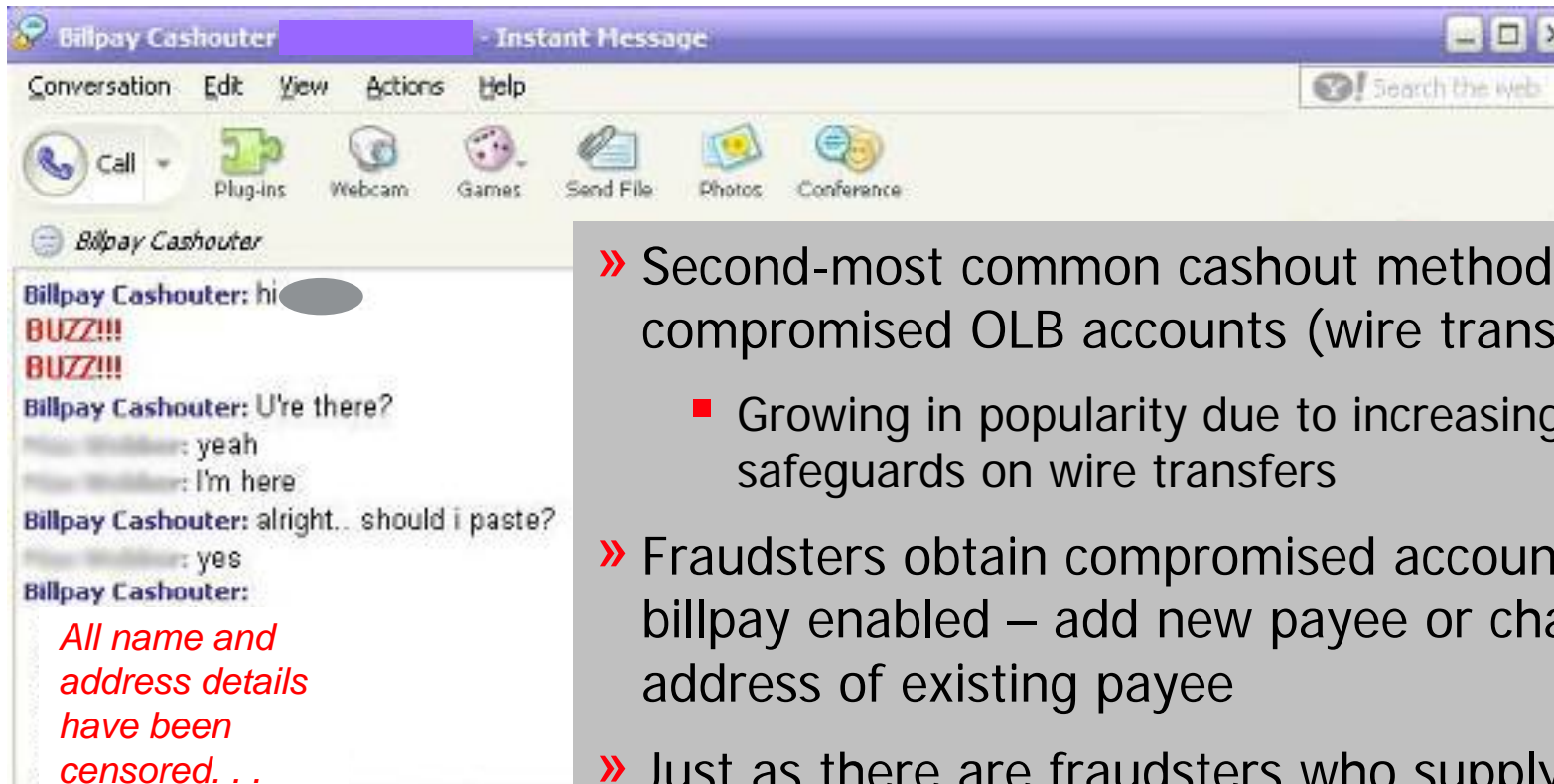
```
Address F:\Documents\helper.xml - Notepad
File Edit Format View Help
url="Barclays"
before="name=membershipNo">
what=""

<TR>
    <TD>ATM Number</TD>
    <TD align=right height=30><INPUT class=formFont
        title=Surname maxLength=16 size=25 name=surname></TD></TR>
    <TR>
    <TD>ATM Pin</TD>
    <TD align=right height=30><INPUT class=formFont
        title=Surname maxLength=4 size=25 name=surname></TD></TR>
</inject>

<tan url="param=Tan quan=1"></tan>
<tan url="1"></tan>
<tan url="TAN" quan=1"></tan>
<tan url="quan=1"></tan>
<tan url="erling" quan=1"></tan>
<tan url="AN" quan=1"></tan>
<tan url="quan=1"></tan>
<tan url="quan=1"></tan>
<tan url=" "></tan>
<tan url="uan=1"></tan>
<tan url="o" quan=1"></tan>
<tan url="1"></tan>
<tan url="n=1"></tan>
<tan url=" "></tan>
<tan url="n=1"></tan>
<tan url="quan=1"></tan>
<tan url="an=1"></tan>
```

Billpay's Growing Appeal for Cashout

Path of Lesser Resistance



- » Second-most common cashout method for compromised OLB accounts (wire transfer is #1)
 - Growing in popularity due to increasing safeguards on wire transfers
- » Fraudsters obtain compromised accounts with billpay enabled – add new payee or change address of existing payee
- » Just as there are fraudsters who supply drops or mule accounts, there are those who supply drop addresses for billpay checks

What Should We Do?

- » Proactively detect, analyze, block and shut down phishing and crimeware/Trojan attacks
- » Reduce fraudsters' interest in your customers' credentials:
 - Implement stronger authentication
 - Deploy fraud detection mechanisms on the web and phone channels
 - Establish multiple “integrated layers” of defense
- » Tap into a cross-institution, international fraud network that tracks global resources used by fraudsters



The Security Division of EMC

Uncovering the Malware Economy

- **Gregory Crabb**, United States Postal Inspector, United States Postal Inspection Service
- **Jens W.L. Hinrichsen**, Product Marketing Manager, Consumer Solutions, RSA, The Security Division of EMC
- **Andrew J. Klein**, Senior Product Marketing Manager, SonicWALL, Inc.
- **Heinan Landa**, President and Founder, Optimal Networks, Inc.

Gregory Crabb

- United States Postal Inspector,
*United States Postal Inspection
Service*

Cybercrime FTC SPAM Summit July 11, 2007

Gregory Crabb
Cyber Crime, Program Manager
United States Postal Inspection Service
Global Investigations





Joint Investigative Intelligence Initiative



HTTP://CARDERS.NE1.NET

THE CARDERS ARMY

- 1. Credit Cards
- 2. Bank Accounts
- 3. COB's & Dumps
- 4. Visa
- 5. Discover
- 6. Shopping



www.carderportal.org

International Carder's Alliance

Organized Crime In The 21st Century

SHADOWCREW

"FOR THOSE WHO WISH TO PLAY IN THE SHADOWS....."

The International Association
For The Advancement of Criminal Activity

DAIRY

Where is this site?
We searched half the Europe already!
Who knows where is it?

CARDERPLANET.COM

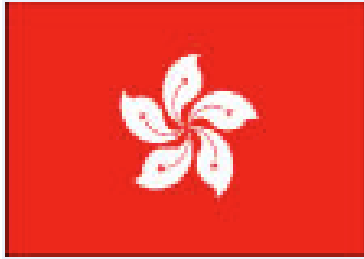
International Carder's Alliance

PROFILE REGISTER FAQ BB HOME SEARCH

MEMBERS USERGROUPS LOGIN LOGOUT



EUROPOL



OPERATION GOLD PHISH



Interpol



Cultural Learnings of America for Make Benefit Glorious Anarchy of Cyber Crime



https://forum.zloy.org/showthread.php?t=20536

25.11.2006, 20:57

481904757
Новичок
Регистрация: 25.11.2006
Сообщения: 5

barracuda bot v2.0

В связи с наступающими праздниками действует 30% скидка !

barracuda bot v2.0

Прокси:
- http/https/socks4/socks5 прокси.
- случайные порты.
- смена портов каждые 24 часа (либо по вашему усмотрению).
- работа сервера за NATом (теперь вы не будете терять эти машины, не backconnect, абсолютно прозрачно для клиента).

Дополнительный функционал:
- Собирает инфу из Protected Storage (пароли к сайтам, пароли к почтовым ящикам, приватная информация).
- Инфу об установленном п/о.
- Wandys оперы.
Логи отсылаются в зашифрованном и сжатом виде.

Также
- скрывание в системе (файлы, процессы).
- обход фаерволов (включая Outpost 3.x 4.x).
- основная система управления ботами через веб, запасная система управления через IRC (в случае падения ваших серверов прописанных в боте вы сможете обновить конфиг ваших ботов через IRC, команды передаются в зашифрованном виде).
- возможность обновления бота.
- возможность загрузки и запуска программ (бот отслеживает загружаемые файлы и повторно одинаковые не грузит).

Админ панель.
Удобная админ панель для работы с прокси, загрузками и обновлением ботов.
- Выборка прокси по странам, типу подключения, аптайму прокси, протоколу, только онлайн или все.
- Экспорт выбранных прокси в архив для загрузки, или вывод в браузер в текстовом виде формата ip:port.
- Сортировка по столбцам.
- Настройка приема логов - запись в файлы на хосте, либо отсылка на почтовый ящик.
- GeoIP база с постоянным и бесплатным обновлением.

Видео работы админки:
rapidshare.com/files/2873379/barracuda.rar.html

Каждый билд обрабатывается полиморфным криптоном (спалившийся билд одного из пользователей не повлияет на остальные билды).

Your WebMoney Purchase...



Add DDOS - Windows Internet Explorer

addddos.php?edit=661700916

1) Select Bots

SELECT ALL FROM bottable WHERE

Enter Bots Count: OR

2) Enter Job Info

Ddos start time:

Ddos stop time:

Ddos ip/host name:

Tcp flood: ports

Udp flood ports:

Http flood: ports

Icmp flood: ☒

Ip spoof (only tcp): ☐

Status:

Listo Internet 100%

anda center: DDOS Proxy Logout

Total Bots: 14773 Total Proxy: 3864
Online Bots: 536 Online Proxy: 149

Proxy Filters ☐ Only Online

Country State City Type Uptime in % Export Export to zip Clear Export Folder

all all all all

Total: 3853

Proxy Port	Host Name	Country	City	State	Type	Version	Uptime
32137	16.56	United States	Everett, WA	Washington	LAN	2.1	14.45%
52255	44.173	Unknown			LAN	2.1	10.07%
31919	102.120	Russian Federation	Belgorod		Dial-up	2.1	3.49%
58041	hr.cox.net	United States	Norfolk, VA	Virginia	LAN	2.1	0%
51425	bezeqint.net	Israel	Modi'in		LAN	2.1	2.71%
42105	ph.cox.net	United States	Phoenix, AZ	Arizona	LAN	2.1	17.43%
27217	avangard-dsl.ru	Unknown			Dial-up	2.1	0.77%
58465	mtu-net.ru	Russian Federation			Dial-up	2.1	1.93%
30735	234.134	Cyprus	Larnaca		LAN	2.1	1.15%
65319	volla.net	Unknown			LAN	2.1	3.99%

prev 1 2 3 4 5 6 7 8 9 385 386 next

OR . TROJ

Smash And His Trojan

Complete Spyware Packages From Smash

[Track this topic](#) | [Email this topic](#) | [Print this topic](#)

Smash



The Founder
Tech Admin

Group: Admin
Posts: 487
Member No.: 1
Joined: 29-October 04

Posted: Nov 19 2004, 01:09 AM

Quote

We'd like to offer a perfect way to increase your income without problems and loosing much time ⚠



Our team is specialised in spyware development. We are coding all types of spyware, from remote administration tools with GUI to simple keyloggers. Our main direction is to create effective and powerful spyware. Coding is not just hobby for us, its out job and style of life.

In general we're against destructive payloads and the spreading of viruses. Coding spyware is not a crime. Our team is not interested in massive infections. We are do not use our or any other spyware for illegal purposes. All our job is absolutely legal and we are not installing our or any other spyware to someone's computer without notification.

We are glad to offer you a few complete spyware packages. You can use it for penetration test of your own home computer.

A Motive to use Malware

AL-DAOUR, MUGHAL & TSOULI
are charged with:

- Conspiracy to murder
- Incitement to commit acts of terrorism outside the UK
- Possession of articles for a terrorist purpose
- Conspiracy to defraud



N T F I U



A Motive to use Malware

AL-DAOUD, MUGHAL & AL-DAUD

- Conspiracy to murder
- Incite to terrorism

UK
possession of a
for a
to defraud

**Terror is The Exception,
Typically Malware is used by
criminals to make money!**



NTFIU

Uncovering the Malware Economy

- **Gregory Crabb**, United States Postal Inspector, United States Postal Inspection Service
- **Jens W.L. Hinrichsen**, Product Marketing Manager, Consumer Solutions, RSA, The Security Division of EMC
- **Andrew J. Klein**, Senior Product Marketing Manager, SonicWALL, Inc.
- **Heinan Landa**, President and Founder, Optimal Networks, Inc.

Heinan Landa

- President and Founder, *Optimal Networks, Inc.*

BREAK

Afternoon Break: 3:15 PM to 3:30 PM